DISEÑO DEL PROCESO DE GESTIÓN DE RIESGOS DE TI DE LA MULTINACIONAL "LA COMPAÑÍA" E IMPLEMENTACIÓN EN EL ÁREA DE OPERACIONES DE TI COLOMBIA

YAMILE ESTHER DUGARTE COLL

UNIVERSIDAD DEL NORTE

DIVISIÓN DE INGENIERÍAS

MAESTRÍA EN GOBIERNO DE TECNOLOGÍA INFORMÁTICA

BARRANQUILLA, COLOMBIA

2017

DISEÑO DEL PROCESO DE GESTIÓN DE RIESGOS DE TI DE LA MULTINACIONAL "LA COMPAÑÍA" E IMPLEMENTACIÓN EN EL ÁREA DE OPERACIONES COLOMBIA

YAMILE ESTHER DUGARTE COLL

PROYECTO DE GRADO

Dirigido por: Ingeniera Margarita Coronell

UNIVERSIDAD DEL NORTE

DIVISIÓN DE INGENIERÍAS

MAESTRÍA EN GOBIERNO DE TECNOLOGÍA INFORMÁTICA

BARRANQUILLA, COLOMBIA

2017

TABLA DE CONTENIDO

TABLA DE GRÁFICAS

1. INTRODUCCIÓN

Este trabajo de grado presenta un proceso de Gestión de Riesgos que guía y apoya la gestión de riesgos para el área de tecnología de “LA COMPAÑÍA”, con base en buenas prácticas de gestión de riesgos. En el desarrollo de los capítulos se evidenciarán los pasos seguidos para la elaboración del proceso unificado para la gestión de riesgos de TI que es el objetivo de este trabajo de Grado.

En primera instancia, se presenta la formulación del problema, objetivos, alcance, limitaciones y la metodología implementada para conocer el estado actual del tema de riesgos en “LA COMPAÑÍA”, y las actividades que se realizaron para el levantamiento del proceso de gestión de riesgos propuesto; en segunda instancia, se presenta el marco general de la gestión de riesgos, donde se establece el contexto, clave para definir el proceso para la gestión del riesgo, debido a que se revisan los objetivos, entorno interno y externo, partes involucradas y una diversidad de criterios que permiten conocer la naturaleza y complejidad de los riegos. Seguidamente se describen cada uno de los subprocesos que garantizan que el riesgo se gestiona eficaz, eficiente y coherentemente: Comunicación y Consulta, Valoración de Riesgo (Identificación, Análisis, Evaluación y Tratamiento del riesgo), y Monitoreo y Revisión; finalmente, se presenta el proceso definido para “LA COMPAÑÍA”, que consiste en la aplicación sistemática de las políticas, los procedimientos y las prácticas de gestión, a las actividades de comunicación, consulta, establecimiento del contexto, y de identificación, análisis, evaluación, tratamiento, monitoreo y revisión del riesgo.

El proceso de gestión de riesgo se definió dentro del Gobierno de TI, con el fin de identificar eventos potenciales que puedan afectar al área de Tecnología, gestionar sus riesgos dentro del riesgo aceptado y proporcionar una seguridad razonable sobre el logro de los objetivos de TI que pueden ser estratégicos (objetivos a alto nivel, alineados con la misión y dándole apoyo), Operaciones (objetivos vinculados al uso eficaz y eficiente de los recursos) o Cumplimiento (objetivos relativos al cumplimiento de leyes y normas aplicables).

2. FORMULACIÓN DEL PROBLEMA

2.1 ANTECEDENTES

“LA COMPAÑÍA” es una multinacional líder en el sector energético, está presente en 25 países, y cuenta con cerca de 20 millones de clientes. En Colombia opera en todo el país atendiendo a más de 4 millones de clientes.

Para dar apoyo y cubrimiento en Colombia, el departamento de Sistemas de Información tiene como misión garantizar procesos de negocio transversales a través de sistemas únicos de gestión para todos los productos, clientes y geografías, mediante la racionalización de las aplicaciones, las plataformas y la optimización de los costes y recursos destinados al desarrollo y mantenimiento de los sistemas. El gobierno y lineamiento estratégico se define en la casa matriz ubicada en el continente Europeo. Sin embargo, dentro de los lineamientos de gobierno no existía un estándar para el manejo y gestión de riesgos.

2.2 PLANTENAMIENTO DEL PROBLEMA

No existía una definición del proceso de riesgo del área de TI, cada división manejaba sus riesgos por separado y no se tenía un control, ni seguimiento estructurado de la gestión de los riesgos. Además, no se contaba con documentación, estándares, ni herramientas para tal fin. Por esta razón, en las últimas auditorias les habían exigido la matriz de riesgos de TI, y que por

no estar estructurada en ese momento, generó no conformidades en los reportes de auditoría.

La gestión del riesgo no es una actividad independiente que se separa de las actividades y los procesos que se ejecutan diariamente. La gestión del riesgo es parte de las responsabilidades de la dirección y una parte integral de todos los procesos de la organización, incluyendo la planificación estratégica, supervisión, aseguramiento y todos los procesos de operaciones, gestión de proyectos y de cambio. Por consiguiente, siendo la tecnología parte de la operación y funcionamiento de la empresa, no puede aislarse de los demás elementos del proceso, dado que tiene importancia y aporte al logro de los objetivos corporativos. Como en todo proceso, existe el factor llamado "riesgo", que es la posibilidad de que ocurra un evento y afecte adversamente el logro de objetivos[1]. Es por esto, que se desarrolló como parte de este proyecto de grado un proceso de gestión de los riesgos que permita identificar oportunidades, evitar o mitigar las pérdidas para el negocio.

2.3 JUSTIFICACIÓN

Las áreas de gobierno de TI tienen dentro de sus objetivos además de alinear la tecnología con los procesos del negocio, la administración apropiada de los riesgos de TI. "LA COMPAÑÍA" como la gran mayoría de compañías a nivel mundial soporta sus procesos operativos y de negocio con TI, generando un alto grado de dependencia de la misma y realiza una alta

[1] FUENZALIDA, Raúl y AMBROSIO, Eduardo. Riesgo tecnológico. Su medición como prioridad para el aseguramiento del negocio [en línea]. <http://www.auditool.org/blog/auditoria-de-ti/827-riesgo-tecnologico-su-medicion-como-prioridad-para-el-aseguramiento-del-negocio> [citado en 20 de Febrero de 2016]

inversión en TI (representada en costos de adquisición, mantenimiento y seguridad). Por lo tanto, TI representa un activo importante para la empresa que debe ser monitoreado y controlado, y los riesgos asociados a estos activos deben ser gestionados de manera adecuada para garantizar el logro de los objetivos estratégicos. Para lograr este objetivo, en conjunto con la división de gobierno de TI de “LA COMPAÑÍA”, se identificó la necesidad de definir y documentar el proceso de gestión de riesgos de TI, objeto de este trabajo de grado.

3. OBJETIVOS

- Definir proceso y estructura metodológica para identificar, evaluar y reducir los riesgos relacionados con TI (cumplimiento, estratégicos, operacionales) que puedan tener un impacto potencial sobre las actividades de TI que soportan las operaciones de negocio, dentro de los niveles de tolerancia establecidos por la organización.

- Integrar la gestión de riesgos de TI bajo una metodología única y aplicable a cada una de las áreas de TI de “LA COMPAÑÍA”.

4. ALCANCE Y LIMITACIONES

4.1 ALCANCE

El alcance incluye la definición del marco general de gestión de riesgos de sistemas de “LA COMPAÑÍA”. Así mismo, incluye la definición del proceso para el análisis, la evaluación de los mismos e implementación de los planes de tratamiento para los riesgos identificados, el monitoreo y seguimiento de los planes de tratamiento y evaluación de riesgos residuales.

Con el desarrollo del proceso y metodología se pretende establecer un marco general para la gestión de riesgos de tecnología donde se definen los lineamientos, criterios y herramientas para la identificación, análisis, evaluación, tratamiento, monitoreo de los riesgos de TI que puedan tener un impacto potencial sobre el área de sistemas y las operaciones de negocio de “LA COMPAÑÍA”. El alcance cubre las siguientes fases:

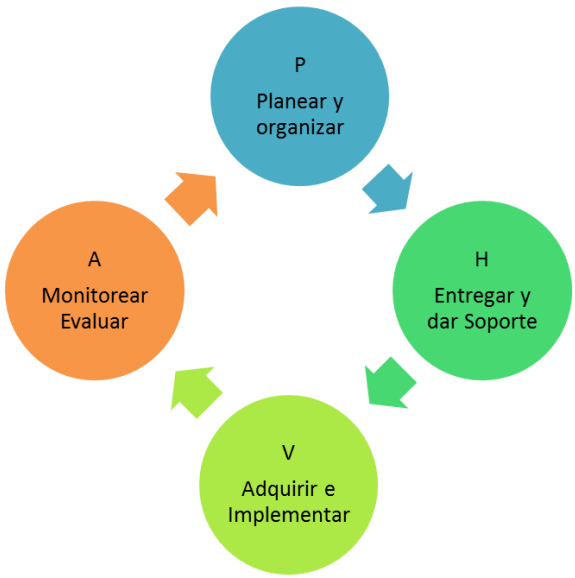
4.1.1 Diagnóstico y Revisión

- Levantamiento de información del proceso actual.
- Revisión de documentación y soportes de proceso existente.
- Identificación de mejoras y oportunidades.

Para esto se utilizó el ciclo PHVA con el fin de realizar el diagnóstico del proceso actual, definir el proceso y subprocesos alineados a políticas de

calidad, los roles y responsabilidades y los controles para el aseguramiento del proceso:

- En la planeación se definieron las actividades, los objetivos y roles involucrados para la revisión de los procesos.
- En el Hacer, se realizó la implementación de lo definido en la Planeación, es decir, toda la Organización se alineó de acuerdo a las definiciones, se conformaron los equipos de trabajo para apoyar la revisión y documentación de los procesos con el enfoque de PHVA y con una metodología definida.
- En la Verificación, se aplicó la validación con los niveles de aprobación definidos.
- En el Actuar, se recibe la retroalimentación de los actores involucrados para un mejoramiento continuo, y se tienen en cuenta para la definición de los nuevos procesos y subprocesos.

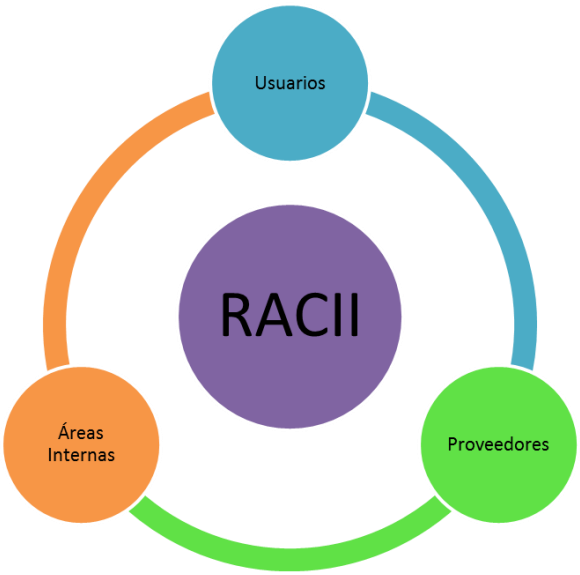


Gráfica 1. Ciclo PHVA

4.1.2 Priorizar y Diseñar

- Definición de la priorización de los procesos.
- Diseño de los procesos definidos.
- Definición de roles y responsabilidades de los procesos.

Se realizó la priorización de actividades para estructurar los procesos, se diseñaron los procesos y se definieron los roles y responsabilidades de los actores en los procesos. Es muy importante esta matriz de roles y responsabilidades porque se establecen unos responsables por la ejecución, monitoreo y periodicidad para el seguimiento del proceso, clave para el éxito de su implementación en “LA COMPAÑÍA”.

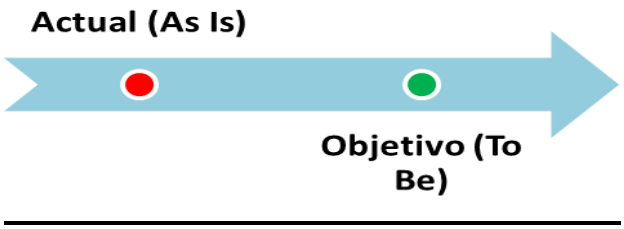


Gráfica 2. RACI - Matriz de Roles y responsabilidades

4.1.3 Implementación

- Definir plan detallado y estrategia de implementación de los procesos para el área de Operaciones de TI.

Se realizó la diagramación del proceso con sus actores, actividades y flujo completo de implementación, se definió un plan de comunicaciones y se implementó para el área de Operaciones de TI.



Gráfica 3. Situación Actual Vs Objetivo

4.2 LIMITACIONES

La implementación se realizó sólo para el área de Operaciones de TI. Además de Operaciones, el departamento cuenta con el área de Gestión de Software y el área de Businness Partners.

5. METODOLOGÍA IMPLEMENTADA

Para el diseño de estos procesos y subprocesos se tuvieron en cuenta las siguientes actividades:

5.1 LEVANTAMIENTO DE INFORMACIÓN DE LOS PROCESOS

En este punto se realizaron reuniones con cada uno de los líderes de las áreas de TI o los responsables de los riesgos de TI, con el fin de identificar las políticas, lineamientos, procesos y/o metodologías de riesgos y las fuentes de captura o formatos utilizados para el registro de los mismos.

5.2 REVISIÓN DE INFORMACIÓN/DOCUMENTACIÓN DE LOS PROCESOS EXISTENTES

Se revisó la documentación con el fin de identificar mejoras alineadas a las mejores prácticas (COBIT, ISO 31000, PMI) y unificar un solo proceso aplicable a todas las áreas de TI de “LA COMPAÑÍA”.

5.3 SECUENCIA Y PRIORIZACIÓN DE ACTIVIDADES

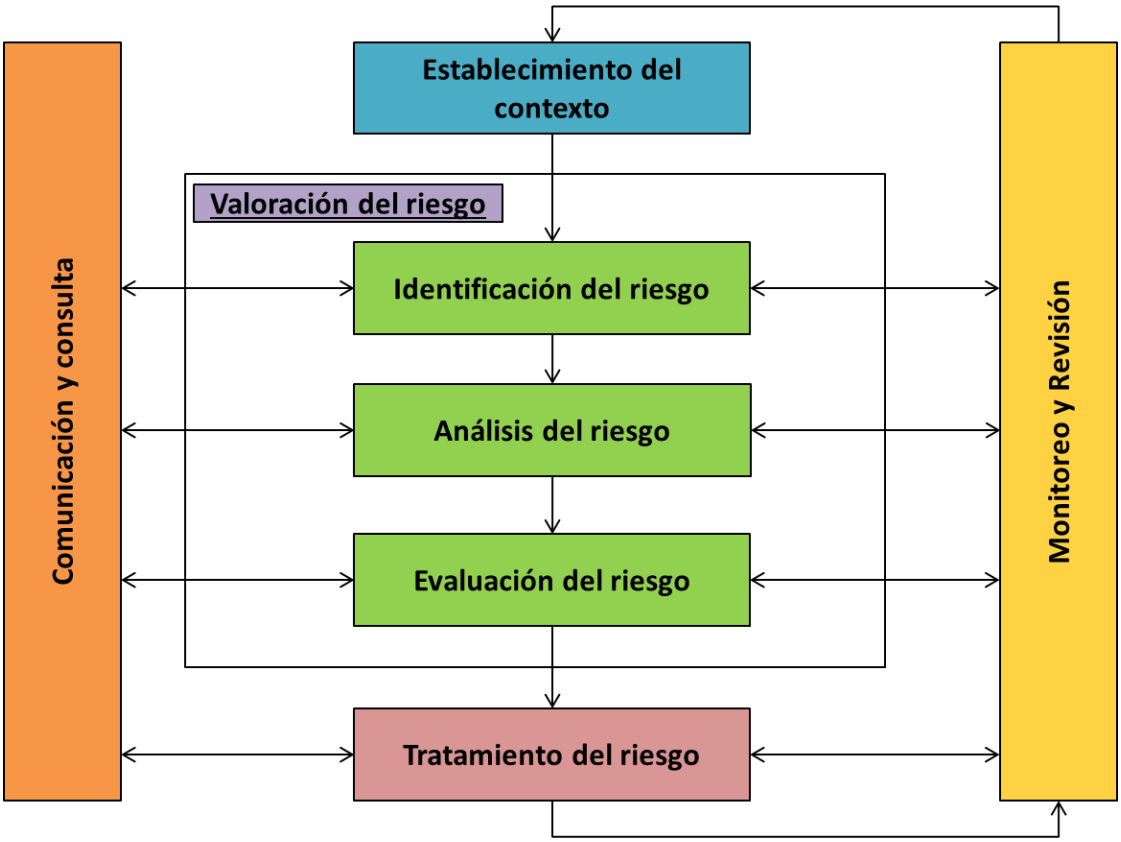
Se definió la secuencia y priorización de las actividades propias del proceso de gestión de Riesgos de TI teniendo en cuenta el proceso estándar NTC-ISO 31000 (Ver Gráfica 4).

5.4 DEFINICIÓN DEL PROCESO

Se definió el proceso de gestión de riesgos para TI, teniendo en cuenta el proceso estándar (Ver Gráfica 4) y los resultados obtenidos en la revisión con los involucrados. Dado que no hay un lineamiento a nivel corporativo todavía en cuanto a la gestión de riesgos, el diseño de estos procesos se fundamentó en enfoques BOTTOM-UP y en las mejores prácticas tales como COBIT 5, ISO 38500, ITIL, ISO31000 y PMI.

Para la definición del proceso se realizó la aplicación sistemática de políticas, procedimientos y prácticas de gestión, a las actividades de comunicación, consulta, establecimiento del contexto, e identificación, análisis, evaluación, tratamiento, seguimiento y revisión del riesgo[2].

[2] Norma Técnica Colombiana NTC ISO 31000 Gestión del Riesgo. Capítulo de términos y definiciones.



Gráfica 4. Proceso Gestión de Riesgos

5.5 IMPLEMENTACIÓN DEL PROCESO

Para la implementación nos enfocamos en el área de operaciones y servicios de TI y con todos los aspectos relacionados con los servicios y sistemas de TI, los cuales pueden producir pérdidas o reducción del valor a la organización. Se definieron los escenarios de riesgos y matriz de riesgos detallada (Herramienta que permite clasificar y visualizar los riesgos, mediante la definición de categorías de consecuencias y de su probabilidad[3]).

[3] SERRA, Carlos. ISO 31000:2009. Herramienta para evaluar la gestión de riesgos [en línea].

5.6 SEGUIMIENTO Y CONTROL

Se definió como parte del proceso de gestión de riesgos, unas actividades para el seguimiento y control y en la matriz de roles y responsabilidades se definió periodicidad de las tareas del proceso, para el continuo monitoreo de los riesgos, implementación de planes de respuesta a los riesgos, monitoreo de riesgos residuales, identificación de nuevos riesgos y evaluación de la efectividad del proceso contra riesgos. Monitorear y revisar también involucra lecciones aprendidas del proceso de gestión de riesgos, a través de la revisión de eventos, los planes de tratamiento y sus resultados.

6. MARCO GENERAL DE GESTIÓN DE RIESGOS DE TI

<http://www.isaca.org/chapters8/Montevideo/cigras/Documents/cigras2011-cserra-presentacion1%20modo%20de%20compatibilidad.pdf> [citado en 11 de Marzo de 2016]

6.1 ESTABLECER EL CONTEXTO DE RIESGOS TI

Se refiere a la comprensión de los antecedentes de “LA COMPAÑÍA” y sus riesgos, el alcance de la gestión de riesgos de las actividades realizadas y el desarrollo de una estructura de gestión de riesgos para las tareas que se ejecutan. En este punto se establecen los parámetros básicos y el alcance dentro del cual, los riesgos de TI deberán ser gestionados[4].

6.1.1 Contexto externo

Ambiente externo en el cual la organización busca alcanzar sus objetivos:

- El ambiente social y cultural, político, legal, reglamentario, financiero, tecnológico, económico y cultural.
- Los impulsores claves y las tendencias que tienen impacto en los objetivos de “LA COMPAÑÍA”.
- Las relaciones con las partes involucradas externas, sus percepciones y valores.

6.1.2 Contexto interno

- Gobierno, estructura de la organización, funciones y responsabilidades.
- Políticas, objetivos, y estrategias implementadas para cumplir los objetivos.

[4] GTC 137 (ISO Guía 73:2009, definiciones)

- Capacidades, entendidas en términos de recursos y conocimientos (presupuesto, tiempo, personas, procesos, sistemas y tecnologías).
- Cultura organizacional.
- Sistemas de información, flujos de información y procesos para la toma de decisiones.
- Normas, lineamientos corporativos y modelos adoptados por la organización.

Dentro de la definición del contexto se deben tener en cuenta las necesidades de la organización tales como:

- Definición de las metas y los objetivos de las actividades de gestión del riesgo.
- Definición de las responsabilidades del proceso para la gestión del riesgo.
- Definir actividad, proceso, función, proyecto, producto, servicio o activo en término de tiempo y ubicación.
- Definición de la metodología de valoración de riesgos.

Se plantea el siguiente contexto de riesgos para “LA COMPAÑÍA”:

Gráfica 5. Contexto de Riesgos de TI

7. PLAN DE COMUNICACIÓN PARA LA GESTIÓN DE RIESGOS TI

La comunicación y la consulta deben ser consideradas en cada etapa del ciclo de gestión de riesgos de TI y se debe desarrollar un plan de comunicaciones para los grupos de interés. Este plan debe direccionar los asuntos relacionados con los riesgos TI y el proceso para gestionarlos. Una apropiada comunicación y consulta busca:

- Mejorar el entendimiento de las personas de los riesgos y el proceso de gestión de riesgos, introduciéndolo en la cultura organizacional de “LA COMPAÑÍA”.
- Asegurar que los diferentes puntos de vista de las partes interesadas son consideradas.
- Asegurar que todos los participantes son conscientes de sus roles y responsabilidades.

8. IDENTIFICACIÓN RIESGOS DE TI

El Objetivo de la identificación de riesgos es desarrollar una completa lista de fuentes de riesgo y eventos que puedan tener un impacto en el logro de los objetivos críticos identificados en el contexto.

8.1 COMPONENTES DE UN RIESGO

Un riesgo está asociado con:

- **Una fuente de riesgo o peligro:** Algo que tiene un potencial intrínseco de perjudicar o de ayudar.
- **Un evento o incidente:** Algo que ocurre de modo que la fuente de riesgo tiene el impacto descrito.
- **Una consecuencia:** Resultado o impacto sobre grupos de interés, procesos y activos.
- **Una causa:** (Qué y por qué) Generalmente una cadena de causas directas y/o relacionadas, de la presencia del peligro o evento que se produzca.
- **Controles** y su nivel de efectividad.
- **Cuándo y dónde** puede ocurrir el riesgo.

Los componentes de un riesgo no deben ser confundidos y se deben identificar de manera separada.

8.2 PROCESO DE IDENTIFICACIÓN

Para desarrollar una lista completa de los riesgos se debe iniciar con la definición del contexto y posteriormente se debe verificar que los riesgos han sido identificados efectivamente en todas las áreas de aplicación, procesos, proyectos y/o servicios de TI. Los pasos a seguir son:

- Identificar las posibles fuentes de riesgo.
- Seleccionar o definir la categoría de riesgos de TI que aplica para el área de aplicación, proyecto y/o servicio para el cual se realizará la identificación de riesgos.
- Revisar los procesos y técnicas con los responsables seleccionados.
- Revisar los procesos y técnicas con los responsables que participarán en la identificación de los riesgos TI para la categoría seleccionada.
- Documentar los resultados en la Matriz Riesgos.

Realizar las siguientes preguntas para cada categoría de riesgos seleccionada:

- ¿Cuál es la fuente para cada riesgo?
- ¿Qué podría suceder?
- ¿Cuál sería el efecto/impacto en los objetivos de “LA COMPAÑÍA”?
- ¿Cuándo, dónde, por qué y probabilidad de que ocurran estos riesgos (positivos o negativos)?
- ¿Quién puede estar involucrado o impactado?
- ¿Qué controles existen actualmente para el tratamiento de estos riesgos?

Después de revisar cada categoría de riesgos, se deben considerar las siguientes preguntas generales:

- ¿Cuál es la fiabilidad de la información?
- ¿Cómo se garantiza que la lista de riesgos está completa?
- ¿Existe la necesidad de una investigación adicional para riesgos específicos?
- ¿Están los objetivos y el alcance cubiertos adecuadamente?
- ¿Está involucrado el personal idóneo en el proceso de identificación de riesgos?

8.3 INFORMACIÓN DE REFERENCIA PARA IDENTIFICAR RIESGOS

El punto de partida para la identificación de riesgos de TI puede ser información histórica de “LA COMPAÑÍA” o de compañías similares y posteriormente dar los debates con los grupos de interés sobre la evolución de la misma. Algunos ejemplos pueden ser:

- Juicio de expertos.
- Entrevistas estructuradas.
- Discusión con grupos focales.
- Reportes de post eventos.
- Experiencia personal o experiencia en otras compañías.
- Resultado de planes de acción de Control Interno, Auditorias, otros.
- Registro histórico, análisis de reporte de incidentes y reportes de avance de los planes de tratamiento de riesgos existente.

9. ANÁLISIS Y EVALUACIÓN DE RIESGOS DE TI

El objetivo del análisis de riesgos es establecer un entendimiento del nivel de riesgo y su naturaleza. También ayuda a establecer prioridades y opciones de tratamiento. El nivel de riesgo es determinado por la combinación de las consecuencias y la probabilidad. Las escalas y métodos más apropiados para las combinaciones, deben ser coherentes con los criterios o elementos claves definidos en el contexto.

La selección del método de análisis es influenciado por el contexto, los objetivos y la disponibilidad de recursos. El proceso de análisis generalmente empieza con una descripción cualitativa que proporciona un entendimiento general de la situación, pero algunos de los riesgos identificados en los procesos, proyectos y/o servicios pueden necesitar una revisión más detallada que puede ser cuantitativa o cualitativa.

9.1 CRITERIOS DE LA EVALUACIÓN DE RIESGOS

Definir los criterios contra los cuales se evaluará el riesgo. Las decisiones sobre si el riesgo debe ser tratado, debe estar basado en criterios operacionales, técnicos, financieros, legales, ambientales, u otros, y depende de las metas y objetivos estratégicos de "LA COMPAÑÍA". Se deben considerar criterios como:

- ***La clase de consecuencias que serán consideradas:*** La consecuencia se determina en base al impacto que tiene el riesgo de TI en los procesos de negocio de "LA COMPAÑÍA".

- ***Cómo se define la probabilidad:*** La probabilidad se determina por el número de veces que ocurre el evento.
- ***Cómo se determina si el nivel de riesgo requiere futuras actividades de tratamiento:*** Una vez aplicado los controles se mide y monitorea el nivel de riesgo residual.

9.2 ANÁLISIS SEMI-CUANTITATIVO O CUANTITATIVO DE RIESGO TI

El nivel de riesgo puede calcularse mediante un método cuantitativo en los casos en que la consecuencia y la probabilidad de ocurrencia se puedan cuantificar. Por ejemplo, la evaluación del riesgo de fraude puede ser cuantitativa, donde la probabilidad se puede expresar numéricamente y los impactos potenciales se miden en términos de impacto monetario.

En muchos casos se utilizan eficazmente métodos relativamente directos, aunque técnicas más especializadas son a veces necesarias. Sin embargo, incluso técnicas cuantitativas sofisticadas pueden tener debilidades y éstas deben ser tenidas en cuenta. Particularmente, los supuestos que son la base de las técnicas cuantitativas deben ser identificados, explicados y entendidos claramente. Cuando resulte un alto nivel de incertidumbre después del análisis, puede ser apropiado señalarlo y revisar el trabajo en una fecha posterior y con la ayuda de un de grupos expertos.

9.3 PREGUNTAS CLAVES EN EL ANÁLISIS DE RIESGOS

Las preguntas clave para realizar el análisis de los riesgos de TI son:

- ¿Qué sistemas actuales pueden prevenir, detectar, mitigar o bajar las consecuencias o las posibilidades de riesgos o de acontecimientos indeseables?
- ¿Qué sistemas actuales pueden incrementar o aumentar las consecuencias o las posibilidades de oportunidades o de acontecimientos beneficiosos?
- ¿Cuáles son las consecuencias o el rango de consecuencias de los riesgos, si llegaran a ocurrir?
- ¿Cuál es la probabilidad o el rango de posibilidad de ocurrencia de los riesgos?
- ¿Cuáles factores pueden aumentar o disminuir la posibilidad o las consecuencias?
- ¿Qué factores adicionales pueden necesitar ser considerados y modelados?
- ¿Cuáles son las limitaciones del análisis realizado y de los supuestos adoptados?
- ¿Qué tan confiable es usted en su juicio o investigación, específicamente en lo referente a la alta consecuencia y la baja probabilidad de riesgos?
- ¿Qué dirige la variabilidad o la incertidumbre?
- ¿Es sólida la lógica detrás de los métodos del análisis?
- ¿Para el análisis cuantitativo, qué ocurre si algunos métodos estadísticos se pueden utilizar para entender el efecto de la incertidumbre y de la variabilidad?

9.4 PROBABILIDAD, IMPACTO Y NIVEL DE RIESGO

Cualquiera que sea el tipo de análisis usado, alguna forma de medición de consecuencias y probabilidad es necesaria. La selección del tipo de escala para llevar a cabo la medición, depende en gran medida de la naturaleza y alcance de las consecuencias, y el nivel de conocimiento y variabilidad de la probabilidad. La relación entre estos dos dependerá de muchos factores que a su vez reflejan la verdadera naturaleza del riesgo y la forma en que se percibe. A continuación se describen las escalas definidas para calcular la probabilidad, consecuencia y el nivel de riesgo en “LA COMPAÑÍA”:

- **Probabilidad:**

  La probabilidad se calculara con los siguientes valores:

  - **Remota (1):** Evento que casi nunca ocurre, una vez cada 5 años o más.
  - **Ocasional (2):** Es posible que ocurra el evento, el periodo de ocurrencia entre un evento y el otro puede ser grande, ocurre entre 1 y 5 años.
  - **Poco frecuente (3):** Es posible que ocurra con frecuencia baja, entre 1 y 4 veces por año.
  - **Frecuente (4):** Existen antecedentes de que el evento ocurrirá dentro de un plazo de tiempo que implique una acción para enfrentarlo pero la frecuencia no es alta, entre 5 y 12 veces por año.
  - **Muy frecuente (5):** El evento se sabe que ocurre con cierto grado de certeza y que la frecuencia es alta, más de 12 veces por año.

- **Impacto:**

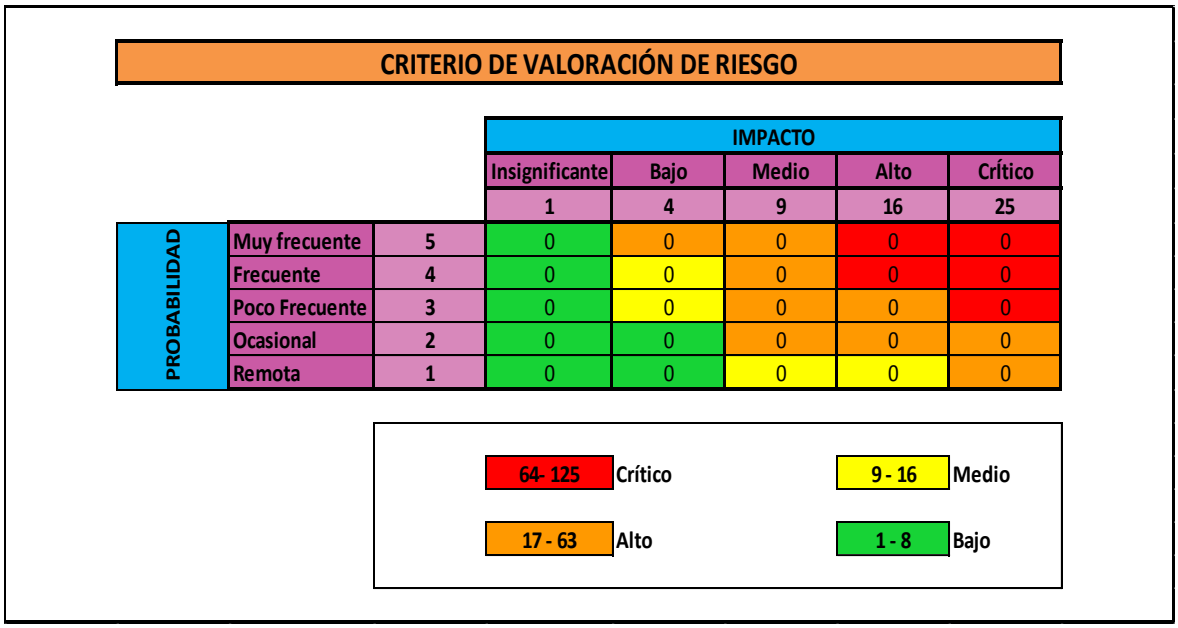
  El impacto se calculará exponencialmente de acuerdo a los siguientes valores:

  - **Insignificante (1) (1^2):** Significa que se trata de un proceso no crítico y la materialización del evento no afecta el proceso ni la operación del negocio.
  - **Bajo (4) (2^2):** Significa que se trata de un proceso de baja criticidad, y la materialización del evento afecta de forma baja el proceso y la operación del negocio.
  - **Medio (9) (3^2):** Significa que se trata de un proceso sensitivo, y la materialización del evento afecta el proceso de negocio, pero no afecta otros procesos.
  - **Alto (16) (4^2):** Significa que se trata de un proceso vital, y la materialización del evento afecta completamente el proceso y la operación del negocio.
  - **Crítico (25) (5^2):** Significa que se trata de un proceso crítico, y la materialización del evento afecta completamente el proceso y la operación del negocio y además afecta otros procesos de negocio.

- **Nivel de riesgo:**

  El nivel de riesgo estará dado por la **Probabilidad X Impacto y** tendrá los siguientes valores:

  - **Bajo:** 1 a 8 (B)
  - **Medio:** 9 a 16 (M)
  - **Alto:** 17 a 63 (A)
  - **Crítico:** 64 a 125 (C)



Gráfica 6. Matriz de valoración de Riesgos TI

9.5 EVALUACIÓN DE RIESGOS

La evaluación de riesgos usa el entendimiento del riesgo alcanzado en el análisis para tomar decisiones sobre futuras acciones. Dichas decisiones pueden determinar:

- Si un riesgo requiere tratamiento,
- Si una actividad debe ser emprendida.
- La prioridad para el tratamiento.

La evaluación de riesgos, consiste en comparar el nivel de riesgo encontrado en el proceso de análisis con los criterios de riesgo establecidos en el contexto.

Los criterios usados para tomar decisiones tienen que ser consistente con el contexto de gestión de riesgos de TI definido, tener en cuenta los objetivos de “LA COMPAÑÍA”, los objetivos del ejercicio de riesgos, y los puntos de vista de los responsables, entre otros. Las decisiones pueden estar basadas en el nivel de riesgo, pero también pueden estar apoyadas en el umbral específico en términos de:

- Consecuencias específicas.
- La probabilidad de eventos específicos o resultados.
- El efecto acumulado de múltiples eventos.
- El rango de incertidumbre para los niveles de riesgo en un determinado nivel de confianza.

10. TRATAMIENTO DE LOS RIESGOS TI

El tratamiento de los riesgos establece las opciones para el tratamiento de los riesgos, la evaluación de dichas opciones y la preparación e implementación de los planes de tratamiento. Las opciones de tratamiento deben ser seleccionadas considerando factores como costo, beneficios, efectividad, y otros criterios relevantes para “LA COMPAÑÍA”. Además se deberá realizar las siguientes acciones:

- **Identificar opciones de tratamiento:** El punto de partida para la identificación de opciones, es a menudo una revisión de las guías para el tratamiento de ese tipo de riesgo. Dentro de las opciones de tratamiento de riesgo se tendrán contempladas las siguientes:
    - **Aceptar:** Si el nivel de riesgo satisface los criterios para su aceptación, no es necesario implementar controles adicionales y el riesgo se puede aceptar.
    - **Mitigar:** Reducir riesgos mediante la selección de controles, de tal forma, que el riesgo residual se pueda evaluar como aceptable.
    - **Transferir:** El riesgo se transfiere a otra de las partes que pueda manejar de manera más eficaz el riesgo particular, dependiendo de la evaluación de riesgos.
    - **Evitar:** Decidir no iniciar o continuar la actividad que lo generó.

- **Evaluar opciones de tratamiento:** En general, una combinación de opciones de tratamiento deberá ser seleccionada para un rango de opciones identificadas. Las opciones seleccionadas deben estar alineadas con los objetivos de la organización y con los criterios de evaluación de los riesgos.

- **Diseño de tratamiento de riesgo:** Se deben tener en cuenta los siguientes pasos:
    - Revisar causas y controles
    - Objetivos del tratamiento
    - Diseño detallado de medidas de tratamiento
    - Comunicación e implementación
    - Análisis costo beneficio

  Para el diseño e implementación de los controles y con el fin de valorar el riesgo residual, se tendrán en cuenta los siguientes valores exponenciales, los cuales están dados según el grado de implementación y gestión del control:
    - **Control no implementado (1) (1^2)**
    - **Control implementado (9) (3^2), no evaluado ni gestionado**
    - **Control gestionado (25) (5^2): (Mejoramiento continuo)**

- **Preparar planes de tratamiento:** El propósito de los planes de tratamiento es documentar la forma como serán implementadas las acciones propuestas. Los planes de tratamiento deben incluir:
    - Acciones propuestas
    - Recursos requeridos
    - Responsabilidades
    - Tiempo
    - Mediciones de desempeño
    - Reporte y monitoreo de requerimientos
    - Riesgos residuales

11. ANÁLISIS Y EVALUACION DE RIESGOS RESIDUALES DE TI

Es el riesgo que sobra después de que las opciones de tratamiento han sido identificadas y los planes de tratamiento han sido implementados. Es importante que las partes interesadas y los encargados de tomar decisiones sean conscientes de la naturaleza y el alcance del riesgo residual. Los riesgos residuales deben estar documentados y se les debe hacer seguimiento y monitoreo. Los riesgo residuales se calcularán en base a: **Riesgo Neto / Estado del Control.**

12. MONITOREO Y SEGUIMIENTO DE LA GESTIÓN DE RIESGOS TI

Las revisión y monitoreo del plan de gestión de riesgos es esencial para garantizar que éste sigue siendo pertinente. Los factores que pueden afectar la probabilidad y las consecuencias de un resultado pueden cambiar con el tiempo y factores que impactan el contexto, así como los factores que inciden en la conveniencia o en el costo de las opciones de tratamiento. Por lo tanto, es necesario repetir el ciclo de gestión del riesgo con regularidad.

Monitorear y revisar también involucra lecciones aprendidas del proceso de gestión de riesgos, a través de la revisión de eventos, los planes de tratamiento y sus resultados:

- Cambios en el contexto de gestión de riesgos TI
- Aseguramiento y monitoreo de la gestión de riesgos
- Mediciones de desempeño de la gestión de riesgos
- Análisis post eventos

13. REGISTRO DE RIESGOS

Cada etapa del proceso de gestión de riesgos debe ser documentado de manera apropiada. De los supuestos, métodos, fuentes de información, análisis, resultados y las razones para las decisiones debe quedar un registro documental.

- **Registro de riesgos:** Para cada riesgo identificado debe existir la siguiente información:
    - Descripción de los riesgos, sus causas e impacto
    - Un resumen de los controles existentes
    - Una evaluación de las consecuencias de los riesgos en caso de que ocurran y la probabilidad de que se produzca la consecuencia, a pesar de los controles
    - Una clasificación del riesgo
    - Una priorización de los riesgos
    - Cronograma de tratamiento de los riesgos y plan de acción
    - Documentos de monitoreo y auditoria
    - Plan de gestión de riesgo

14. REPORTES DE DESEMPEÑO DE LOS PLANES DE TRATAMIENTO

En esta etapa se realiza los reportes de desempeño, que se generan por el monitoreo realizado.

15. PROCESO DE RIESGOS DE TI

15.1 ALCANCE DEL PROCESO

El alcance del proceso de riesgos comienza con el establecimiento del marco general de gestión de riesgos de sistemas de “LA COMPAÑÍA”; así mismo incluye el análisis, la evaluación de los mismos e implementación de los planes de tratamiento para los riesgos identificados, el monitoreo y seguimiento de los planes de tratamiento y evaluación de riesgos residuales. Actividades anteriormente descritas desde el capítulo 6 al 14 del presente trabajo de grado.

15.2 GLOSARIO DEL PROCESO[5]

- **Análisis del riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel del riesgo.
- **Consecuencia:** Resultado de un evento.
- **Criterios del riesgo:** Términos de referencia considerados al evaluar la importancia de un riesgo.
- **Evaluación del riesgo:** Proceso de comparación de los resultados del análisis de riesgos con los criterios del riesgo.
- **Evento:** Presencia o cambio de un conjunto particular de circunstancias.
- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

[5] GTC 137 (ISO Guía 73:2009, Definiciones).

- **Identificación del riesgo:** Proceso para encontrar, reconocer y describir el riesgo.
- **Nivel de riesgo:** Magnitud de un riesgo o de una combinación de riesgos, expresada en términos de la combinación de consecuencias y su probabilidad.

- **Perfil del riesgo:** Descripción de cualquier conjunto de riesgos.

- **Probabilidad:** Posibilidad de que suceda algo.

- **Propietario del riesgo:** Persona o entidad con la responsabilidad de rendir cuentas y con la autoridad para gestionar un riesgo.

- **Riesgo:** Efecto de incertidumbre sobre los objetivos.

- **Riesgo residual:** Riesgo remanente después del tratamiento de riesgos.

- **Tratamiento del riesgo:** Proceso para modificar el riesgo.

- **Valoración del riesgo:** Proceso global de identificación del riesgo, análisis del riesgo y evaluación del riesgo.

15.3 POLÍTICAS DEL PROCESO

Con el desarrollo de este proceso se pretende establecer un marco general para la gestión de riesgos de tecnología donde se definen los lineamientos, criterios y herramientas para la identificación, análisis, evaluación, tratamiento, monitoreo de los riesgos de TI que puedan tener un impacto potencial sobre el área de sistemas y las operaciones de negocio de “LA COMPAÑÍA”.

15.4 ROLES Y RESPONSABILIDADES

Los roles definidos para el proceso de Gestión del Riesgo son:

ROLES	RESPONSABILIDADES
BUSINESS PARTNER	• Liderar, coordinar, y velar por la correcta implementación del proceso de Riesgos de "LA COMPAÑÍA". • Proporcionar los criterios y herramientas para la evaluación de los Riesgos. • Asesorar en el análisis y selección de las alternativas más adecuadas para la transferencia o retención de riesgos de TI. • Realizar seguimiento al cumplimiento de los planes de tratamiento de los riesgos críticos de TI. • Realizar observaciones y/o sugerencias respecto de los planes de tratamiento de riesgos críticos de TI.
RESPONSABLE DE GOBIERNO DE TI	• Apoyar a los responsables de los riesgos en la identificación de las causas y la elaboración de los planes de tratamiento. • Consolidar la información enviada por los responsables de los riesgos. • Realizar el reporte del estado de las acciones y el porcentaje de avance del plan de tratamiento consolidado de los riesgos TI. • Coordinar la realización de los ajustes necesarios al plan de tratamiento. • Reportar el avance de las acciones y asegurar el monitoreo y seguimiento periódico al desempeño de los planes de tratamiento y del ciclo de gestión de riesgos TI en general. • Definir acciones correctivas, preventivas y planes de mejora cuando sean requeridas para asegurar el cumplimiento con el menor retraso posible de los planes de tratamiento establecidos.
LIDER DEL ÁREA DE SISTEMAS	• Establecer un contexto de Gestión de Riesgos TI para el desarrollo del ciclo de gestión de riesgos • Verificar, aprobar los resultados de cada una de las etapas del ciclo de gestión de riesgos. • Socializar y divulgar los resultados de cada etapa del ciclo de gestión de riesgos. • Asegurar el diseño e implementación de un plan de tratamiento para los riesgos críticos de TI identificados. • Designar las personas responsables para la elaboración y ejecución de los planes de tratamiento de los riesgos críticos de TI. • Asegurar los recursos (humanos, tiempo, presupuesto, técnicos, otros) para la ejecución de los planes de tratamiento. • Hacer seguimiento periódico al estado de las acciones y el porcentaje de avance de los planes de tratamiento.
ANALISTA DE RIESGOS	• Apoyar al Responsable de Gobierno de TI en las tareas requeridas en el ciclo de la gestión de riesgos de TI. • Apoyar al responsable de Gobierno de TI en la gestión del tratamiento de riesgos.

16.1 MÉTRICAS DEL PROCESO

El proceso apoya la consecución de un conjunto de principales metas de TI:

META TI	MÉTRICAS RELACIONADAS
Riesgos de negocio relacionados con los Riegos de TI gestionados	• Número de incidentes significativos relacionados con TI que no fueron identificados en la evaluación de riesgos. • Porcentaje de procesos de negocio críticos y programas de negocio habilitados por TI cubiertos por la evaluación de riesgos. • Porcentaje de evaluaciones de riesgo de la empresa que incluyen los riesgos relacionados con TI.

16.2 DESARROLLO DE ACTIVIDADES

El proceso está compuesto por unas actividades que permiten Identificar, evaluar y reducir los riesgos de TI de forma continua, dentro de niveles de tolerancia establecidos por “LA COMPAÑÍA”. A continuación se detallan paso a paso las actividades del proceso de Gestión de riesgos, describiendo las tareas, responsable de su ejecución y periodicidad:

ACTIVIDAD	DESCRIPCIÓN / TAREAS	RESPONSABLE	PERIODICIDAD
1. Establecer el marco general de Gestión de Riesgos de TI	A través de la definición del contexto de gestión de riesgos donde se establecen los parámetros básicos y el alcance dentro de los cuales los riesgos de TI deberán ser gestionados. Establecer el marco general de gestión de riesgos TI se refiere a la comprensión de los antecedentes de "LA COMPAÑÍA" y sus riesgos, el alcance de la gestión de riesgos de las actividades emprendidas y de las tareas a seguir. Los pasos a seguir para la elaboración del contexto de gestión de riesgos TI se especifican en ESTABLECER EL CONTEXTO DE RIESGOS TI	Jefe BP´s / Responsable Gobierno TI	Una vez al año
2. Diseñar plan de comunicaciones y consulta	Elaborar un plan de comunicaciones para direccionar los asuntos relacionados con el ciclo de gestión de riesgos TI y el proceso para gestionarlos, con el objetivo de fomentar una cultura orientada hacia la administración de los riesgos, establecer un lenguaje común y mantener actualizadas a las personas involucradas en la gestión de riesgos de TI sobre las estrategias y actividades. Algunas consideraciones para la elaboración del Plan de Comunicaciones se especifican en PLAN DE COMUNICACIÓN PARA LA GESTIÓN DE RIESGOS DE TI	Responsable Gobierno TI	Se realiza en la etapa inicial y se actualiza en cada etapa del ciclo de gestión de riesgos TI
3. Seleccionar área de aplicación proyecto y/o servicio	Seleccionar las opciones disponibles en el contexto de gestión de riesgos de TI dentro de las cuales los riesgos pueden aparecer y los criterios de evaluación de acuerdo con el proceso, proyecto y/o servicio del área de sistemas a la cual se va aplicar el ciclo de gestión de riesgos TI.	BP´s / Líder de Operaciones / Líder ADM / Responsable de Gobierno TI	Por demanda, como mínimo una vez por año

ACTIVIDAD	DESCRIPCIÓN / TAREAS	RESPONSABLE	PERIODICIDAD
4. Identificar riesgos	Elaborar una lista completa de fuentes de riesgo y eventos que puedan tener un impacto en el logro de los objetivos estratégicos y/o en los procesos de negocio que soporta el área de sistemas de “LA COMPAÑÍA”. Los pasos a seguir para el desarrollo de la etapa de Identificación de riesgos se especifican en IDENTIFICACIÓN RIESGOS DE TI.	BP´s / Líder de Operaciones / Líder ADM / Responsable de Gobierno TI	Por demanda, como mínimo una vez por año
5. Aprobar y comunicar lista de riesgos identificados	El responsable de gobierno de TI y el Business Partner deberán verificar y aprobar los resultados de esta etapa así como socializar y divulgar los mismos.	Jefe BP´s / Responsable Gobierno TI	Por demanda
6. Designar responsables de los riesgos	Para la elaboración de planes de tratamiento y monitoreo de riesgos “LA COMPAÑÍA” deberá designar un ejecutor para cada una de las acciones y/o controles incluidas en el plan de tratamiento para los riesgos críticos de TI.	BP´s / Líder de Operaciones / Líder ADM / Responsable de Gobierno TI	Por demanda
7. Analizar y evaluar los riesgos	En esta etapa se establece un entendimiento del nivel de riesgo y su naturaleza para tomar decisiones sobre futuras acciones, dichas decisiones pueden determinar: • Si un riesgo requiere tratamiento, • Si una actividad debe ser emprendida, y • La prioridad para el tratamiento. Los pasos a seguir y las herramientas para el desarrollo de la etapa de análisis y evaluación de riesgos se especifican en ANALISIS Y EVALUACIÓN DE RIESGOS DE TI.	Business Partner / Líder de Operaciones / Líder ADM / Responsable de Gobierno TI	Por demanda

ACTIVIDAD	DESCRIPCIÓN / TAREAS	RESPONSABLE	PERIODICIDAD
8. Describir cualitativamente los riesgos	El proceso de análisis generalmente empieza con una descripción cualitativa que proporciona un entendimiento general de la situación de los riesgos identificados.	Jefe BP´s / Líder de Operaciones / Líder ADM / Responsable de Gobierno TI	Por demanda
9. Determinar probabilidad, consecuencias y nivel de riesgo	Cualquiera que sea el tipo de análisis usado, alguna forma de medición de consecuencias y probabilidad es necesaria. La selección del tipo de escala para llevar a cabo la medición, depende en gran medida de la naturaleza y alcance de las consecuencias, el nivel de conocimiento y variabilidad de la probabilidad. La relación entre estos dos dependerá de muchos factores que a su vez reflejan la verdadera naturaleza del riesgo, la forma en que se percibe y la forma de describir el nivel del riesgo dependerá del tipo de análisis realizado. Los pasos a seguir para determinar probabilidad, consecuencias y nivel de riesgo se especifican en PROBABILIDAD, IMPACTO Y NIVEL DE RIESGO. En el caso de hacer análisis cuantitativo previo, se debe utilizar como insumo la información generada en esa actividad.	BP´s / Líder de Operaciones / Líder ADM / Responsable de Gobierno TI	Por demanda
10. Priorizar riesgos TI	De acuerdo a la valoración dada a cada uno de los riesgos identificados se debe elaborar una lista ordenada de los riesgos y sus causas identificando los riesgos críticos con el fin de optimizar recursos y hacer planes de tratamiento efectivos.	Jefe BP´s / Responsable de Gobierno TI	Por demanda

ACTIVIDAD	DESCRIPCIÓN / TAREAS	RESPONSABLE	PERIODICIDAD
11. Identificar, evaluar y seleccionar opciones de tratamiento	Para cada uno de los riesgos críticos identificados se debe diseñar un plan de tratamiento. Las opciones de tratamiento deben ser seleccionadas considerando factores como costo, beneficio, efectividad y otros criterios relevantes. Algunas de las opciones de tratamiento incluyen: Eliminar/Evitar, mitigar/reducir, asumir y/o transferir. Los pasos a seguir para el desarrollo de esta etapa, se especifican en TRATAMIENTO DE LOS RIESGOS DE TI	BP´s / Líder de Operaciones / Líder ADM / Responsable Gobierno TI / Analista de Riesgos	Por demanda
12. Asesorar en la selección de opciones de tratamiento	El responsable de gobierno de TI, y el analista de riesgos debe acompañar y asesorar la selección de opciones de tratamiento requeridas para los riesgos críticos identificados y establecer las acciones y/o controles, que se consideren efectivas, eficaces, eficientes, convenientes y adecuadas.	Responsable de Gobierno TI / Analista de riesgos	Por demanda
13. ¿Las opciones de tratamiento incluyen retención o transferencia del riesgo?	Si dentro de los planes de tratamiento se incluyen opciones de retención o transferencia de riesgos se debe buscar la asesoría y el soporte del responsable de Gobierno de TI y del analista de riesgos.	Responsable de Gobierno TI / Analista de riesgos	Por demanda
14. Asesorar en la selección de esquemas de transferencia y retención de Riesgos	El analista de riesgos debe analizar y seleccionar los esquemas alternativos y tradicionales, de transferencia de riesgos más adecuados para “LA COMPAÑÍA” (ej. pólizas de seguros).	Analista de riesgos	Por demanda

ACTIVIDAD	DESCRIPCIÓN / TAREAS	RESPONSABLE	PERIODICIDAD
15. Preparar y/o modificar planes de tratamiento	El propósito de los planes de tratamiento es documentar la forma como serán implementadas las opciones elegidas para cada uno de los riesgos críticos de TI. Los planes de tratamiento deberán incluir: • Acciones propuestas • Recursos requeridos • Responsabilidades • Tiempo • Mediciones de desempeño • Reporte y monitoreo de requerimientos • Riesgos residuales Los pasos a seguir para la preparación y/o modificación de los planes de tratamiento se especifican TRATAMIENTO DE LOS RIESGOS TI.	BP´s / Responsable de Gobierno TI / Business Partner / Líder de Operaciones / Líder ADM/ Analista de riesgos	Por demanda
16. Revisar y aprobar el plan de tratamiento definitivo	El responsable de gobierno de TI y el Jefe de BP´s, deberán revisar el plan definitivo, asegurando que este sea pertinente, adecuado y suficiente.	Jefe BP´s / Responsable de Gobierno TI	Por demanda
17. ¿Los planes de tratamiento son suficientes?	Determinar si los planes de tratamiento definidos son suficientes para disminuir las consecuencias y/o probabilidad de ocurrencia de los riesgos críticos de TI identificados. Si son suficientes, se deben asignar los recursos necesarios. Si no, se debe identificar otras alternativas de tratamiento.	Jefe BP´s / Responsable de Gobierno TI	Por demanda

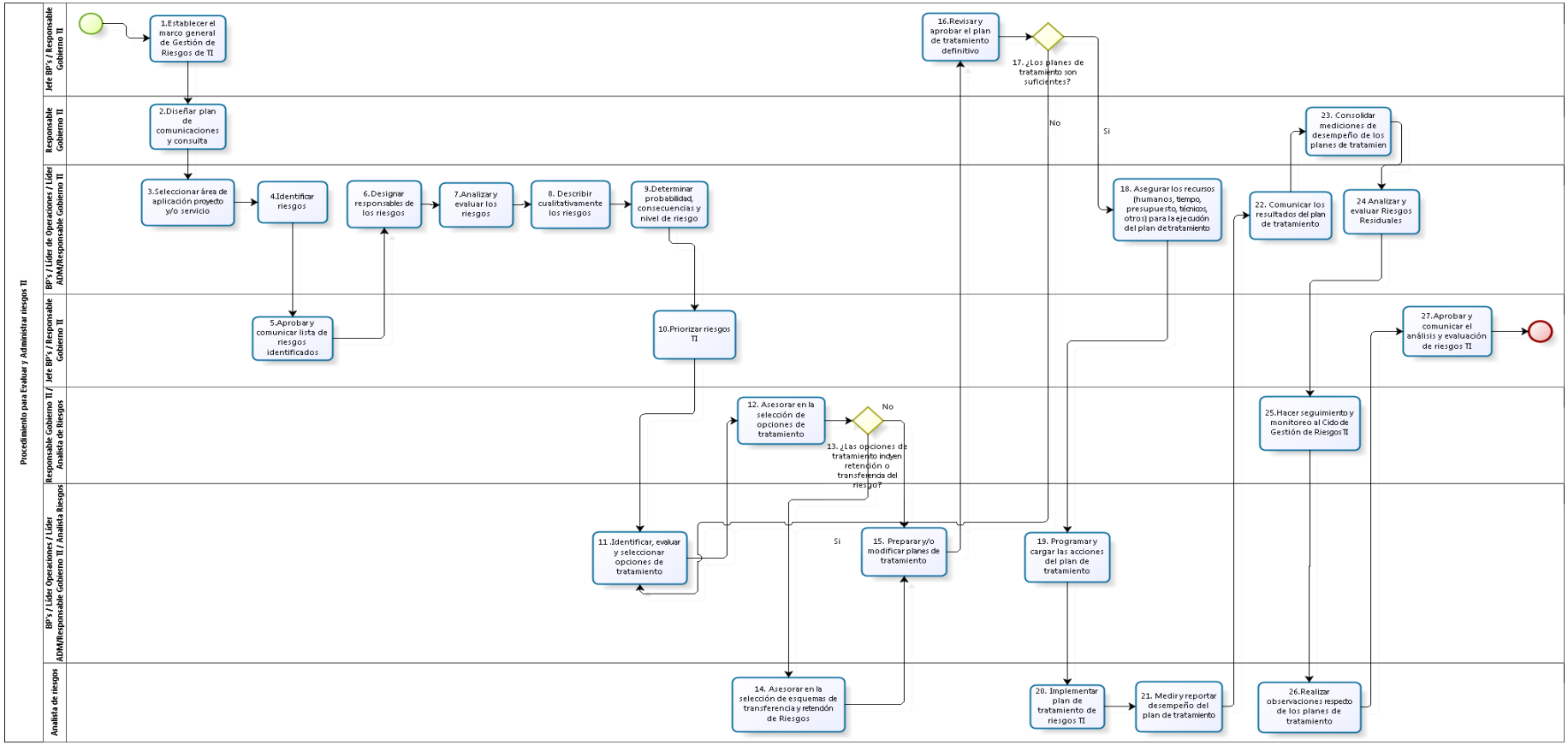
ACTIVIDAD	DESCRIPCIÓN / TAREAS	RESPONSABLE	PERIODICIDAD
18. Asegurar los recursos (humanos, tiempo, presupuesto, técnicos, otros) para la ejecución del plan de tratamiento	Si los planes de tratamiento son suficientes se deberán asignar los recursos necesarios para el desarrollo o ejecución de las acciones definidas. El presupuesto para la implementación de los planes de tratamiento deberá estar definido como una partida dentro del presupuesto del área de Tecnología.	BP´s / Líder de Operaciones / Líder ADM / Responsable de Gobierno TI	Por demanda
19. Programar y cargar las acciones del plan de tratamiento	Las acciones definidas en los planes de tratamiento de riesgos críticos de TI deberán ser registradas en una base de datos diseñada para tal fin.	Responsable de Gobierno TI / BP´s / Líder de Operaciones / Líder ADM / Analista de riesgos	Por demanda
20. Implementar plan de tratamiento de riesgos TI	Las personas designadas como ejecutores del plan de riesgo, son los encargados de poner en marcha el plan de acción definido para cada riesgo dentro del plan de tratamiento.	Analista de riesgos	Por demanda
21. Medir y reportar desempeño del plan de tratamiento	Cada ejecutor deberá reportar el cumplimiento y la efectividad de las acciones implementadas para los riesgos críticos que le fueron asignados.	Analista de riesgos	Por demanda

ACTIVIDAD	DESCRIPCIÓN / TAREAS	RESPONSABLE	PERIODICIDAD
22. Comunicar los resultados del plan de tratamiento	Los líderes del área de Tecnología deberán comunicar periódicamente el resultado de la implementación de las acciones establecidas en los planes de tratamiento de acuerdo con el plan de comunicaciones diseñado en la etapa inicial del ciclo de gestión de riesgos de TI.	BP´s / Líder de Operaciones / Líder ADM / Responsable de Gobierno TI	Por demanda
23. Consolidar mediciones de desempeño de los planes de tratamiento	El responsable de Gobierno de TI deberá consolidar los planes de tratamiento e informar a los responsables las acciones implementadas para los riesgos críticos identificados.	Responsable Gobierno TI	Por demanda
24. Analizar y evaluar Riesgos Residuales	Una vez que los planes de tratamiento han sido implementados, es importante que los responsables de los riesgos sean conscientes de la naturaleza y el alcance del riesgo residual. Los riesgos residuales deberán estar documentados y se les debe hacer seguimiento y monitoreo. Los pasos a seguir para realizar el análisis y evaluación de riesgos residuales se especifican en ANÁLISIS Y EVALUACION DE RIESGOS RESIDUALES DE TI.	BP´s / Líder de Operaciones / Líder ADM / Responsable de Gobierno TI	Por demanda

ACTIVIDAD	DESCRIPCIÓN / TAREAS	RESPONSABLE	PERIODICIDAD
25. Hacer seguimiento y monitoreo al Ciclo de Gestión de Riesgos TI	El ciclo de gestión de riesgos TI deberá ser revisado y monitoreado permanentemente para garantizar su pertinencia, dado que los factores que pueden afectar la probabilidad y las consecuencias de un resultado pueden cambiar, así como los factores que inciden en la conveniencia o en el costo de las opciones de tratamiento. Se debe asegurar un esquema de seguimiento y monitoreo a los planes de tratamiento de los riesgos críticos, así como la actualización de los listados de riesgos cuando éstos lo requieran.	Responsable Gobierno TI / Analista de riesgos	Mensualmente
26. Realizar observaciones respecto de los planes de tratamiento	El analista de riesgos podrá hacer observaciones y/o sugerencias respecto a los planes de tratamiento de riesgos críticos de TI, las cuales deben ser tenidas en cuenta en los diferentes procesos, proyectos y/o servicios y modificar los planes de tratamiento si se requiere.	Analista de riesgos	Por demanda
27. Aprobar y comunicar el análisis y evaluación de riesgos TI	El Responsable de gobierno de TI y el Jefe de BP´s, deberán verificar y aprobar los resultados de esta etapa así como socializar y divulgar los mismos.	Jefe BP´s / Responsable Gobierno TI	Por demanda

16.3 DIAGRAMA DEL PROCESO

Diagrama del Proceso de Gestión de Riesgos de TI[6] (Anexo 1):



[6] Anexo 1. Diagrama del Proceso de Gestión de Riesgos de TI

16. RESULTADOS

Se ha obtenido un proceso estándar para la gestión de riesgos de tecnología que permitió conocer el contexto de la empresa, el estado inicial de la gestión de riesgos, identificar las oportunidades de mejora, priorizar las actividades y adaptar las mejores prácticas y estándares para obtener una metodología única y aplicable a cada una de las áreas de TI de “LA COMPAÑÍA”.

Al aplicar el proceso, se construyó la matriz de riesgos para el área de Operaciones de TI, estableciendo la gestión de riesgos dentro del gobierno, estrategia y cultura de TI. La matriz de riesgos desarrollada, permitió la identificación de escenarios de riesgos para el área de Operaciones de TI, identificar los controles existentes, valorar los riesgos, proponer acciones de tratamiento de riesgos residuales y establecer responsables para el monitoreo y control de los riesgos. Esta matriz de riesgos resultante del proceso, debe ser revisada y actualizada periódicamente, debido a que los riesgos pueden cambiar y las acciones de tratamiento pueden requerirse en otros casos, dependiendo de las situaciones que se presenten.

A continuación se presenta le Matriz de Riesgos[7] (Anexo 2) y las respectivas valoraciones de riesgo inherente, riesgo de exposición y riesgo residual.

[7]Anexo 2. Matriz de Riesgos y Valoraciones de Riesgos.

Nomenclatura	Evento	Causa	Consecuencia (Afectación)	Valoración del riesgo									Tratamiento del riesgo							
				Probabilidad de ocurrencia	Impacto	Riesgo Inherente	Criticidad Inherente	Controles Existentes	Probabilidad de ocurrencia	Impacto	Riesgo Exposición	Criticidad Exposición	Tratamiento	Descripción del control	Estado del control	Probabilidad de ocurrencia	Impacto	#¿NOMBRE?	Criticidad residual	Aceptación del riesgo
RK1	Impacto en la Información	Dado que actualmente no se realizan restauraciones de las copias de respaldo de la aplicación y no se cuentan con ambientes de pruebas para dichas restauracioness	Es posible que en el momento que se desee restaurar el backup, éste se encuentre dañado o no se pueda garantizar la integridad de la información	1	9	9	M	Bitácora de Backups	1	9	9	M	Mitigar	Se deben generar controles que permitan garantizar la integridad y consistencia de los backup realizados.	9	1	9	9	M	T
RK2	Interrupción en la continuidad del servicio	Dado que la base de datos no cuenta con esquemas de alta disponibilidad	Es posible que se presenten interrupciones en el servicio de facturación, cobros, recaudo, lecturas entre otros procesos de negocio que soporte la solución ERP	1	9	9	M	Backups y copias de respaldo periódicos	1	9	9	M	Mitigar	Se deben definir esquemas de alta disponibilidad para las bases de datos de las aplicaciones que esten acordes con las necesidades del negocio.	1	1	9	9	M	T
RK3	Sanciones por incumplimiento en la ley de protección de datos	Dado que actualmente no se tienen identificados los datos personales que se manejan en el sistema ERP	Es posible que generen sanciones(Economicas, reputacionales) por incumplimiento de la ley	2	9	18	A	En proceso proyecto de levantamiento de información de dastos personales	1	9	9	M	Mitigar	Se deben identificar las bases de datos personal que se registraran en las bases de datos de la SIC.	9	1	9	9	M	T
RK4	Documentación obsoleta o desactualizada	Dado que la documentación no se actualiza a medida que se realizan cambios en las aplicaciones	* Es posible que no se cuente con el soporte y mantenimiento adecuado para garantizar la disponibilidad de las mismas * Es posible que se generen errores de configuración de las aplicaciones	3	16	48	A	En proceso proyecto de estándarización de proceso de desarrollo y gestión de la configuración	2	16	32	A	Mitigar	Dentro de las aprobaciones de los cambios se deben incluir actividades que permitan garantizar las modificaciones a nivel documental.	9	1	16	16	M	T
RK5	Falta de aseguramiento de los procesos de TI	Dado que no se revisan periodicamente los procesos de TI	Es posible que estos no se encuentren alineados con las necesidades del negocio y de TI, afectando la operación de los servicios	4	4	16	M	Se está realizando revisión de procesos y actualización.	2	4	8	B	Mitigar	Se deben definir revisiones periodicas a los procesos de TI. De dichas revisiones se deben generar actas o evidencias.	9	2	4	8	B	A
RK6	Impacto de recurso claves de TI	Dado que no se cuentan con planes y procesos de backup de recursos claves de TI	Es posible que se afecte el servicio y la disponibilidad de las aplicaciones afectando la operativa	1	1	1	B	Se están documentando las tareas de cada recurso.	1	1	1	B	Mitigar	Se deben definir mecanismos de pares o tecnicas de transferencia de conocimiento.	9	1	1	1	B	A
RK7	Impacto de continuidad en las operaciones	Dado que no se cuenta con un Centro de Procesamiento Alterno	Es posible que al fallar el principal se vea afectada toda la operativa del negocio	1	25	25	A	No existe control	1	25	25	A	Mitigar	Se debe definir e implementar un DRP.	1	1	25	25	A	I
RK8	Equipos obsoletos o software desactualizado	Dado que se cuenta con equipos de más de 5 años de antigüedad y que adicionalmente existe software que ya no tiene soporte ni mantenimiento	Es posible que se presenten errores de configuración o vulnerabilidades que afecten la disponibilidad, integridad y confidencialidad de la información	1	9	9	M	Se está realizando un inventario de los equipos y software obsoleto para tomar decisiones al respecto.	1	9	9	M	Mitigar	Actualización de las máquinas e ifdentificación de los incidentes más comunes por este tipo de sucesos.	1	1	9	9	M	T
RK9	Transferencia de conocimiento	Dado que la documentación existente del la mesa de servicio es limitante	Es posible que en el cambio de proveedor se presenten afectaciones en los tiempo de solución de los casos	3	16	48	A	No existe control	3	16	48	A	Mitigar	Se deben definir procesos de servicio de "La Compañía" para que cualquier proveedor que ingrese nuevo siga los lieneamientos corporativos en estos procesos.	1	1	16	16	M	T
RK10	Continuidad del negocio	Dado que actualmente "La Compañía" no cuenta con un BCP definido	Es posible que ante algun acontecimiento que impacte el servicio no se tenga identifcados y priorizados los procesos de negocio a recuperar, ni se tengan definidas estas estrategias de recuperación	1	25	25	A	No existe control	1	25	25	A	Mitigar	Se debe definir e implementar un BCP.	1	1	25	25	A	I

VALORACIÓN DE RIESGO INHERENTE	VALORACIÓN DE RIESGO EXPOSICIÓN	VALORACIÓN DE RIESGO RESIDUAL

CRITERIO DE VALORACIÓN DE RIESGO INHERENTE

Probabilidad		Impacto: Insignificante (1)	Bajo (4)	Medio (9)	Alto (16)	Crítico (25)
Muy frecuente	5	0	0	0	0	0
Frecuente	4	0	1	0	0	0
Poco Frecuente	3	0	0	0	2	0
Ocasional	2	0	0	1	0	0
Remota	1	1	0	3	0	2

Criticidad	Valoración
Bajo	1
Medio	4
Alto	5
Critico	0
Total	**10**

64- 125	Crítico	9 - 16	Medio
17 - 63	Alto	1 - 8	Bajo

CRITERIO DE VALORACIÓN DE RIESGO EXPOSICIÓN

Probabilidad		Impacto: Insignificante (1)	Bajo (4)	Medio (9)	Alto (16)	Crítico (25)
Muy frecuen	5	0	0	0	0	0
Frecuente	4	0	0	0	0	0
Poco Frecue	3	0	0	0	1	0
Ocasional	2	0	1	0	1	0
Remota	1	1	0	2	0	2

Criticidad	Valoración
Bajo	2
Medio	4
Alto	4
Critico	0
Total	**10**

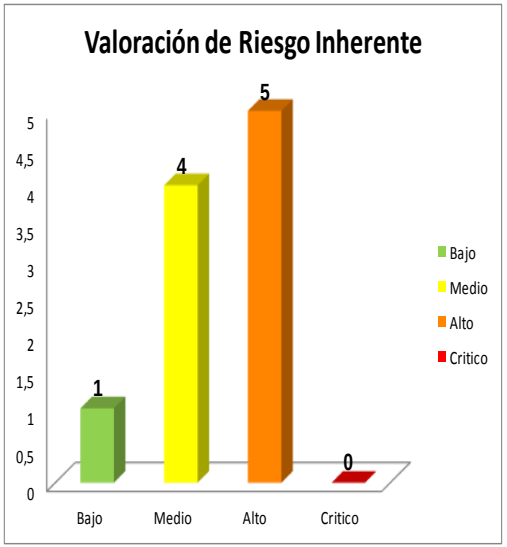
64- 125	Crítico	9 - 16	Medio
17 - 63	Alto	1 - 8	Bajo

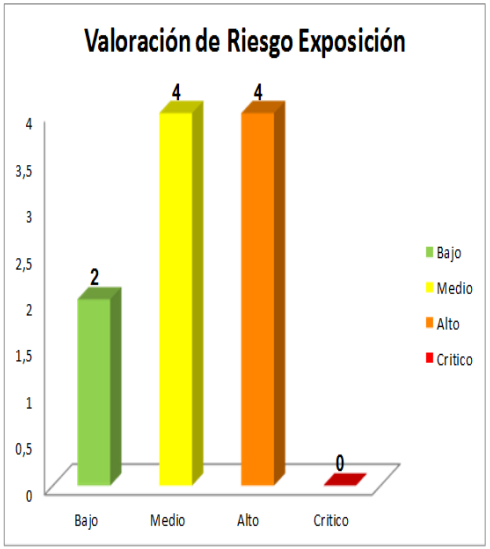
CRITERIO DE VALORACIÓN DE RIESGO RESIDUAL

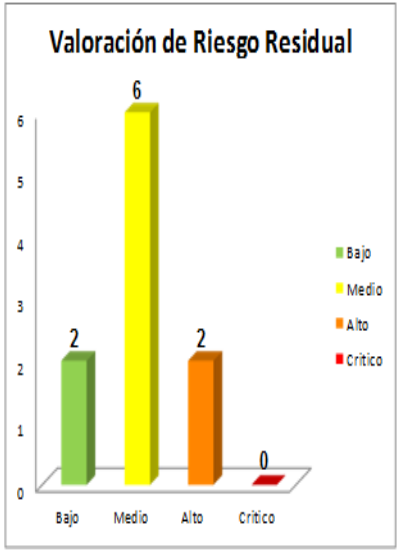
Probabilidad		Impacto: Insignificante (1)	Bajo (4)	Medio (9)	Alto (16)	Crítico (25)
Muy frecuen	5	0	0	0	0	0
Frecuente	4	0	0	0	0	0
Poco Frecue	3	0	0	0	0	0
Ocasional	2	0	1	0	0	0
Remota	1	1	0	2	2	2

Criticidad	Valoración
Bajo	2
Medio	6
Alto	2
Critico	0
Total	**10**

64- 125	Crítico	9 - 16	Medio
17 - 63	Alto	1 - 8	Bajo







La implementación de este proceso, permitió a “LA COMPAÑÍA”:

- Ser consciente de la necesidad de identificar, priorizar y tratar los riesgos de TI. Al implementarlo en el área de Operaciones de TI, se identificaron algunos riegos relacionados con las otras áreas que pusieron en descubierto muchas oportunidades para mejorar los controles y minimizar las pérdidas.
- La Gerencia de TI, identificó la necesidad de replicar este proceso de Gestión de Riesgos en todas las áreas de TI, y definir el rol de Analista de Riesgos, clave para la gestión de riesgos dentro del área de TI.
- Cumplir con requisitos legales y reglamentarios, que permiten asegurar las operaciones.
- Asignar y usar eficazmente los recursos para el tratamiento del riesgo de TI.
- Mejorar la prevención de pérdidas operativas, gestión de incidentes, mejorar las decisiones de respuesta a los riesgos y adelantarnos a los eventos que puedan afectar las operaciones e intereses de “LA COMPAÑÍA”, para asegurar una operación proactiva
- Reducir las sorpresas e improvisaciones y establecer una base confiable para la toma de decisiones y la planificación.
- Identificar aquellos efectos adversos específicos vinculados a cada proceso, lo que permite el desarrollo de medidas efectivas para su tratamiento.
- Desarrollo de las actividades que permitan asegurar que razonablemente se cumplan los objetivos y metas de TI.
- Mejorar el aprendizaje organizacional y el gobierno de TI.
- El proceso de gestión de riesgos y la matriz de riesgos, permitirán en próximas auditorías presentar la gestión de riesgos de TI, mostrando herramientas para aumentar la probabilidad de alcanzar los objetivos, alineando el riesgo aceptado y la estrategia.

17. CONCLUSIONES

El proceso de gestión de riesgos de TI propuesto, permitió establecer una guía para que las áreas de TI puedan seguir paso a paso un grupo de actividades que les permitirán darle gestión a los riesgos que antes no realizaban, exponiendo a la compañía a pérdidas y posibilidad de no lograr los objetivos.

Mediante el desarrollo de este trabajo de grado, se brindó a “LA COMPAÑÍA” un proceso unificado para apoyar la identificación, priorización, valoración, tratamiento, seguimiento y control de los riesgos, con base en buenas prácticas de gestión de los mismos. Este proyecto de grado permitió elaborar un proceso que puede ser adaptable a otras empresas de la misma o diferente naturaleza de “LA COMPAÑÍA”, lo que permite que se convierta en un referente importante para futuros trabajos de grado en gestión de riesgos de TI.

Este proceso propuesto y la guía paso a paso, contaron con el estudio de diferentes literaturas, normas, estándares, y otros trabajos de este tipo relacionados en la bibliografía, que permiten proponer una metodología clara y aplicable, que permitirá a cada una de las áreas de TI de “LA COMPAÑÍA” seguirla y con la ayuda de las preguntas y estructura de cada uno de los capítulos, obtener la lista de riesgos y darle la gestión adecuada para minimizar el impacto en las operaciones, disminuyendo la subjetividad de las técnicas para la valoración de los riesgos.

Con base en los pasos propuestos en el proceso de gestión de riesgos, fue posible construir la matriz de riesgos para el área de Operaciones de TI, disminuyendo el tiempo que se emplea normalmente en realizar el análisis y evaluación de los riesgos, además asegurando el cumplimiento de cada una de las actividades que permiten la adecuada gestión de los riesgos e involucramiento de los stakeholders necesarios para asegurar el entendimiento y aprendizaje organizacional en este tema.

Es importante que estas herramientas que permiten apoyar el proceso de gestión de riesgo se revisen y actualicen periódicamente, con el fin de asegurar su eficacia y eficiencia. Por eso, fue importante establecer los roles y responsabilidades, y la periodicidad de cada una de las actividades, lo que no deja dudas, acerca de las tareas y responsabilidades de las partes involucradas. El proceso y la matriz de riesgos entregada como parte de este trabajo de grado, requiere revisiones y evaluaciones periódicas orientadas a detectar debilidades y oportunidades de mejora, nuevos riesgos, cambio en los identificados, nuevos controles, entre otros factores, para su actualización constante.

La gestión de riesgos es un elemento importante de la estrategia corporativa y del proceso de toma de decisiones de las empresas, es por esto, que este proceso entregado se convierte en una herramienta más para apoyar el cumplimiento de las estrategias y directrices de TI y de “LA COMPAÑÍA” en general.

18. REFERENCIAS BIBLIOGRÁFICAS CONSULTADAS

AS/NZS 4360:1999. Estándar Australiano. Administración de Riesgos

ANDRADE, Deisy Johanna y MOSQUERA, Luisa Fernanda. Proyecto de Investigación, Innovación y Desarrollo Tecnológico en Gestión de Riesgos en proyectos software. Universidad del Cauca, Marzo 2013.

BALLESTER Fernández, José Manuel. GOBIERNO CORPORATIVO TIC. Objetivos y Metodología para su implantación. [En línea].

<www.isacamty.org.mx/archivo/Standard_ISO38500.pdf> [citado en 21 de Noviembre de 2016].

CANEO, Pablo. Cobit 5 para riesgos. Metodología. Una visión general [en línea] (2015).

<http://www.isaca.org/chapters8/Montevideo/cigras/Documents/CIGRAS2015/CIGRAS-2015.09.09-07-Cobit%205%20para%20Riesgos.%20Metodologia.%20Una%20vision%20general-Pablo%20Caneo.pdf> [citado en 25 de Febrero de 2016].

CAÑAS Pacheco, Luis Ernesto. Gestión de riesgos de negocio. Desarrollo e Implementación de Sistemas de Gestión de Riesgos. Banco Central de Reserva de El Salvador. Documentos Ocasionales No. 2009-01. [En línea]. <https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=6&

cad=rja&uact=8&ved=0ahUKEwjawZO347XSAhVlHGMKHTuGAZ8QFgg-MAU&url=http%3A%2F%2Fwww.bcr.gob.sv%2Fbcrsite%2Fdownloads.php%3Fdta%3D773&usg=AFQjCNGWK60f2WIA1nnuXT_LMpfbRakxQQ&sig2=g8eLmVI5mgi-ozfOutCR4w&bvm=bv.148073327,bs.1,d.cGc> [citado en 10 de Noviembre de 2016].

COBIT 5 (2013). For Risk

COBIT 5 (2012). Un Marco de Negocio para el Gobierno y la Gestión de la Empresa. 2012.

COBIT 5 (2012). Procesos Catalizadores.

FRAYSSINET, Delgado Maurice. Taller de Gestión de Riesgos [en línea]. <http://www.ongei.gob.pe/docs/Taller_gestion_de_riesgos.pdf> [citado en 10 de Marzo de 2016].

FUENZALIDA, Raúl y AMBROSIO, Eduardo. Riesgo tecnológico. Su medición como prioridad para el aseguramiento del negocio [en línea]. <http://www.auditool.org/blog/auditoria-de-ti/827-riesgo-tecnologico-su-medicion-como-prioridad-para-el-aseguramiento-del-negocio> [citado en 20 de Febrero de 2016].

GBEGNEDJI, Gladys. Gestión de los Riesgos del Proyecto [en línea] (2013). <https://whatisprojectmanagement.wordpress.com/2013/01/24/gestion-de-los-riesgos-del-proyecto/> [citado en 21 de Febrero de 2016].

GTC 137 (ISO Guía 73:2009, Definiciones)

Norma Técnica Colombiana NTC ISO 31000 Gestión del Riesgo. Capítulo de términos y definiciones. 2009.

PEÑA IBARRA, José Angel y RICO, Salomón. Un vistazo general de COBIT 5 for Risk [en línea] (2013). <http://www.isaca.org/chapters7/Monterrey/Events/Documents/20133110_COBIT_5_for_Risk.pdf> [citado en 25 de Febrero de 2016].

PMBOK 5th Edición (2013). A Guide to the Project Management Body of Knowledge.

RITEGNO, Eduardo Oscar. Gestión de Riesgos de TI, un enfoque desde el marco de trabajo COBIT 5 [en línea]. <https://www.iaia.org.ar/files/164-Eduardo%20Oscar%20Ritegno.pdf> [citado en 10 de Marzo de 2016]

SERRA, Carlos. ISO 31000:2009. Herramienta para evaluar la gestión de riesgos [En línea].

<http://www.isaca.org/chapters8/Montevideo/cigras/Documents/cigras2011-cserra-presentacion1%20modo%20de%20compatibilidad.pdf> [citado en 11 de Marzo de 2016]

VACAS, María Carolina. Taller de Gestión de Riesgos. [En línea]. www.pminuevocuyo.org/.../PMI%20-%20**Taller**%20de%20**Riesgos**%20092012%20v2_0.pdf [citado en 11 de Diciembre de 2016].